PCSF Congress of Chairs

Cyber Security Combined Glossary Project

Duplicate Terms

From

Seventeen Cyber Security Glossaries

Version of

March 28, 2007

This handout will give you insight into one major activity of the Congress of Chairs, the Combined Glossary Project. The basic concept of this project is to collect glossaries from as many process control-related cyber security standards groups as possible and combine them. To date, we have posted on our Web site combined glossaries for seventeen groups:

- AGA 12
- API 1164
- CIDX Report on Cybersecurity Vulnerability Assessment Methodologies, version 2.0, November 2004
- FIPS Pub 200
- IEC TC57 WG15: IEC 62351-2 Data and Communications security Glossary of Terms, 1st Committee Draft for Vote (CDV) Version 3 (not submitted yet), September 2006
- ISA Comprehensive Dictionary of Instrumentation and Control
- ISA SP99
- NERC Glossary of Terms Used in Reliability Standards, effective April 1, 2005
- NERC Cyber Security Standards Cip-002-009
- NERC Security Guidelines for the Electricity Sector: Physical Security – Substations, October 15, 2004
- NERC Threat Alert System and Cyber Response Guidelines for the Electricity Sector: Definitions of Cyber Threat Alert Levels, Version 2.0, October 8,2002
- NERC Security Guidelines for the Electricity Sector: Patch Management for Control Systems, Version 1.0, May 5, 2005
- NERC Security Guidelines for the Electricity Sector: Control System – Business Network Electronic Connectivity, Version 1.0, May 3, 2005

- NIST SP800-53
- PCSRF Field Device Protection Profile
- SD6, SC 27 N 2776
- Microsoft Security Glossary, Published October 29, 2002, Updated December 19, 2005

To see the most current version, visit the PCSF Congress of Chairs Web site at :

https://www.pcsforum.org/groups/59/

and click on “LIBRARY.”

This document identifies the terms that differed as of the date at the top of this page. Note that discussions are under way to align some of these terms and it is expected that many of the differences will be eliminated in the near future. Any group that has a glossary that it would like to contribute should contact Bill Rush at -

William.Rush@comcast.net

Duplicates of Definitions of Process Control Terms and Acronyms

Using These Definitions to Save Effort and Simplify Standards Development

Some of the primary goals of the Congress of Chairs are to avoid duplication of effort, to simplify standards development work, and to avoid the emergence of incompatible or conflicting standards. The Combined Glossary, posted on the PCSF Web site, lists all of the cyber security terms that have been combined from the various glossaries that have been contributed. The Combined Glossary is designed to achieve these goals by providing a single collection of definitions of terms and acronyms drawn from a variety of sources. It is our hope that this collection will be useful to several groups, including the following:

- Standards groups that have not yet developed their own glossary. Using this collection will both save effort and assure agreement with the terminology used by other groups.
- Standards groups that have completed – or are developing – their glossary are invited to submit their definitions to the Congress of Chairs for inclusion of their work in this document. This will save others the effort of developing terms and reduce the odds of some other group's using these same terms in a different sense.
- Standards groups that have already developed and published terms that differ from those that are published by other groups in different documents will be made aware of the differences as a minimum. Identifying such instances allows people to recognize the differences as a minimum. The Congress of Chairs also provides a forum that may allow harmonization of terminology by jointly developing a single definition of the terms.

This document is the subset of terms from the Combined Glossary that are duplicates of one another. Please consult the PCSF Web site for the most recent version of this document, because new glossaries are added periodically and some terms that differed originally have been modified for agreement.

The Definitions Come From Several Sources

Below is a numbered list of sources from which the term/acronym was taken. Sources for definitions are shown in the third column of the table of Definition of Terms and Definition of Acronyms. If the same term has more than one definition, all definitions are given, along with the source. There is no significance to the order in which differing definitions of the same term are arranged. To provide a standard method of selecting which definition is given first, the terms are arranged in the order in which they were received. This list will expand as new glossaries are submitted to the Congress of Chairs for inclusion.

1 FIPS PUB 140-2, (2001): Security Requirements for Cryptographic Modules, Section 2, Glossary of terms and acronyms, National Institute of Standards and Technology.

2 IEEE 100: The Authoritative Dictionary of IEEE Standards Terms", 7th ed.: Institute of Electrical and Electronics Engineers.

3 DNP Technical Bulletin 2002-x, Message Authentication Object.

4 NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation.

5 RFC 793: Transmission Control Protocol, September 1981.

6 RFC 2828: Internet Security Glossary.

7 Menezes, Alfred J., van Oorschot, Paul C., and Vanstone, Scott A. (1997) Handbook of Applied Cryptography, CRC Press.

8 Schneier, Bruce: Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

9 FIPS PUB 198, (2002): The Keyed-Hash Message Authentication Code (HMAC).

10 AGA 12, Part 1, Cryptographic Protection of SCADA Communications

11 ISA-SP99, Manufacturing and Control Systems Security

12 CNSS Instruction No. 4009, National Information Assurance Glossary, May 2003

12* CNSS Instruction No. 4009, Adapted

13 API Standard 1164

14 FIPS PUB 200 (2005): Minimum Security Requirements for Federal Information and Information Systems

15 NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems

16 NIST SP 800-37

17 OMB Circular A-130, Appendix III

18 44 U.S.C., Sec. 3542

19 44 U.S.C., Sec. 5125(b)

20 41 U.S.C., Sec. 403

21 FEA Program Management Office

22 40 U.S.C., Sec. 11331

23 44 U.S.C., Sec. 3502

24 40 U.S.C., Sec. 1401

25 FIPS 199

26 NIST SP 800-18

27 47 C.F.R., Part 64, App A

28 OMB Memorandum 02-01

29 OMB Memorandum 03-22

30 NIST SP 800-30

31 44 U.S.C., Sec. 3544

31 NIST SP 800-53

32 CIDX Report on Cybersecurity Vulnerability Assessment Methodologies, version 2.0, November 2004

33 ISA Comprehensive Dictionary of Instrumentation and Control, edited by W. H. Cubberly, 1988

34 NERC Glossary of Terms Used in Reliability Standards (adopted by NERC Board of Trustees: February 8, 2005; effective date: April 1, 2005)

35 NERC Cyber Security Standards Cip-002-009, November 8, 2005

36 NERC Security Guidelines for the Electricity Sector: Physical Security – Substations, October 15, 2004

37 NERC Threat Alert System and Cyber Response Guidelines for the Electricity Sector: Definitions of Cyber Threat Alert Levels, Version 2.0, October 8, 2002

38 NERC Security Guidelines for the Electricity Sector: Patch Management for Control Systems, Version 1.0, May 5, 2005

39 NERC Security Guidelines for the Electricity Sector: Control System – Business Network Electronic Connectivity, Version 1.0, May 3, 2005

40 PCSRF Field Device Protection Profile

41 IEC 62351-2 Data and Communications Security Glossary of Terms, 1st Committee Draft for Vote (CDV) Version 3 (not submitted yet), September 2006 [Editor's note: This document draws definitions from ATIS/INFOSEC-99, FIPS 140-2, FS-1037C, IETF RFC2828, ISA SP99, ISO/IEC, NIST, and WIKI.]

42 SD6, SC 27 N 2776

43 Microsoft Security Glossary, Published October 29, 2002, Updated December 19, 2005

44 IEEE P1711 Trial Use Standard for a Protocol for Cyber Security of Substation Serial Links

Definition of Terms

Term	Definition	Source
Access Control	The restriction of entry or use, to all or part of, any physical, functional, or logical unit.	10
Access Control	1. Prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [ISO/IEC 18028-2: 2006-02-01] 2. Protection of resources against unauthorized access; a process by which use of resources is regulated according to a security policy and is permitted by only authorized system entities according to that policy. [RFC 2828] 3. A service feature or technique used to permit or deny use of the components of a communication system. 4. A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device. 5. The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device. 6. Limiting access to information system resources only to authorized users, programs, processes, or other systems. 7. That function performed by the resource controller that allocates system resources to satisfy user requests. [FS-1037C]	41
Access Control	The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based. See also access control list and accesscontrol entry.	43
Accountability	A property that ensures that the actions of an entity may be traced uniquely to that entity.	10
Accountability	1. The property that ensures that the actions of an entity may be traced uniquely to the entity [ISO/IEC 7498-2] 2. The property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions. [RFC2828]	41
Accountability	The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.	14, 15, 16
Accreditation	Formal declaration by the responsible management approving the operation of an automated system in a particular security mode using a particular set of safeguards. Accreditation is the official authorization by management for the operation of the system, and acceptance by that management of the associated residual risks. Accreditation is	42

Term	Definition	Source
	based on the certification process as well as other management considerations. {ISO/IEC WD 15443-1 (11/2001)]	
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.	14, 15, 17
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, operational, and technical controls. [NIST]	41
Agency	See Executive Agency.	15
Agency	Any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, but does not include: (i) the Government Accounting Office; (ii) the Federal Election Commission; (iii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (iv) government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.	14, 23
Asset	An entity that may have value to someone. Assets may be tangible or intangible. Examples are people, a facility, materials, equipment, information, business reputation, an activity or operation such as manufacturing, the environment, and the community.	32
Asset	Anything that has value to the organization. [ISO/IEC PDTR 13335-1 (11/2001)] Anything that has value to the organization, its business operations and theoir continuity. [ISO/IEC 17799: 2000]	42
Assets	Information or resources to be protected by the countermeasures of a TOE. [ISO/IEC 15408-1: 1999]	42
Assurance	In the context of security: Grounds for confidence that a deliverable meets its security objectives. [ISO/IEC 15408-1] Note: this definition is generally accepted within the security community; within ISO the more generally used definition is: Activity resulting in a statement giving confidence that a product, process or service fulfils specified requirements. [ISO/IEC Guide 2]	41
Assurance	Grounds for confidence that an entity meets its security objectives. [ISO/IEC 15408-1: 1999] Performance of appropriate activities or processes to instil confidence that a deliverable meets its security objectives. [ISO/IEC WD 15443-1 (11/2001)]	42

Term	Definition	Source
Asymmetric cipher	Cipher based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption [ISO/IEC 18033-1].	41
Asymmetric Cipher	Alternative term for asymmetric encipherment system. [ISO/IEC WD 18033-1 (12/2001)]	42
Asymmetric Key Pair	A pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO/IEC 9798-1: 1997-08-01]	41
Asymmetric Key Pair	A pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)] Pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO/IEC WD 18033-1 (12/2001)]	42
Attack	Attempt to gain unauthorized access to a system's services, resources, or information, or the attempt to compromise an Information System's integrity, availability, or confidentiality. [CNSS]	12
Attack	Hostile action taken by an adversary to obtain access to an asset and use it to achieve their objectives.	32
Attack	1. An attempt to destroy, expose, alter, or disable an Information System and/or information within it or otherwise breach the security policy. [ISO/IEC FDIS 18043: 2006-03-14] 2. An attempt to violate computer security. Note: An example of an attack is malicious logic. [2382-pt.8] 3. [An] intentional act of attempting to bypass one or more of the following security controls of an information system (IS): non-repudiation, authentication, integrity, availability, or confidentiality. [INFOSEC-99]	41
Attack	An attempt to exploit an IT system vulnerability. [ISO/IEC DTR 15947 (10/2001)]	42
Attack	A deliberate attempt to compromise the security of a computer system or deprive others of the use of the system.	43
Authentication	A process that establishes the origin of information, or validates an	10

[1] The AGA 12 Task Group found that "Authentication" has two distinct meanings. One is authentication of one cryptographic module (CM) to another, simply establishing that the module is talking to the module to which it believes it is talking. The other meaning of authentication is establishing that the CM indeed is

Term	Definition	Source
	entity's identity[1].	
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [CNSS]	12
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.	14, 15
Authentication	The process used to verify user identity.	39
Authentication	1. [Any] Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [INFOSEC-99] [After JP 1-02] 2. A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator. [JP 1-02] 3. Evidence by proper signature or seal that a document is genuine and official. [JP 1-02] [FS-1037C] 4. A process that establishes the origin of information, or determines an entity's identity. [RFC2828] 5. the provision of assurance of the claimed identity of an entity [ISO/IEC 10181-2:1996]	41
Authentication	The provision of assurance of the claimed identity of an entity. [ISO/IEC TR 13335-4: 1999]	42
Authentication	The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital signatures, smart cards, biometric data, and a combination of user names and passwords.	43
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.	15
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information. [ISO/IEC TR 13335-1:1996 (3.3) monolingual (English) only]	41
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information. [ISO/IEC PDTR 13335-1 (11/2001)]	42

really associated with domain (i.e., user defined name) identity with which it is claimed to be associated.

Term	Definition	Source
Authorization	The right or a permission that is granted to a system entity to access a system resource.	10, 12
Authorization	(1.) An “authorization” is a right or a permission that is granted to a system entity to access a system resource. (2.) An “authorization process” is a procedure for granting such rights. (3.) To “authorize” means to grant such a right or permission. (See: privilege.) [RFC2828]	41
Authorization	The process of granting a person, computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access, which is verified through authentication.	43
Authorized User	In security, a user who may, according to an organization’s security policy, perform an operation. [After CC-99] [FS-1037C]	41
Authorised User	A user who may, in accordance with the TSP, perform an operation. [ISO/IEC 15408-1: 1999]	42
Availability	The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.	10, 11
Availability	Ensuring timely and reliable access to and use of information.	14, 15, 18
Availability	The number of hours in the reporting period less the total downtime for the reporting period divided by the number of hours in the reporting period (expressed in percent).	33
Availability	1. the property of being accessible and usable upon demand by an authorized entity [ISO/IEC 13335-1:2004] 2. The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them. [RFC2828]	41
Availability	The property of being accessible and usable upon demand by an authorized entity. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Availability	The property of a system or a system resource that ensures it is accessible and usable upon demand by an authorized system user. Availability is one of the core characteristics of a secure system.	43
Back Door	*Synonym* for Trapdoor. A hidden software or hardware mechanism, usually created for testing and troubleshooting, that may be used to circumvent computer security. [ATIS]	41
Back Door	A hardware or software-based hidden entrance to a computer system that can be used to bypass the system’s security policies.	43

Term	Definition	Source
Backup	A copy of information to facilitate recovery, if necessary.	10
Back-up	1. Equipment which is available to complete an operation in the event that the primary equipment fails. 2. A copy of a computer diskette which protects against destruction or loss of the original.	33
Bandwidth	The rate at which a data path (e.g., a channel) carries data, measured in bits per second.	10
Bandwidth	1. A group of consecutive frequencies constituting a band that exists between limits of stated frequency attenuation. A band is normally defined as more than 3.0 decibels greater than the mean attenuation across the band. 2. A group of consecutive frequencies constituting a band that exists between limits of stated frequency delay.	33
Bandwidth	Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second. [RFC2828]	41
Block	A group of contiguous characters formed for transmission purposes.	10
Block	1. A set of things, such as words, characters, or digits, handled as a unit. 2. A collection of contiguous records recorded as a unit, blocks are separated by interblock gaps, and each block may contain one or more records. 3. In data communication, a group of contiguous characters formed for transmission purposes. The groups are separated by interblock characters. 4. A group of physically adjacent words or bytes of a specified size particular to a device. The smallest system-addressable segment on a mass-storage device in reference to I/O. See also cylinder block; block-and-tackle.	33
Block	A bit-string of length L_1, i.e., the length of the first input to the round-function. [ISO/IEC FDIS 9797-2 (09/2000), ISO/IEC CD 10118-3 (11/2001)] A string of bits of length $L_\bullet$·, which shall be an integer multiple of 16. [ISO/IEC 10118-4: 1998] A bit-string of length n. [ISO/IEC 9797-1: 1999] String of bits of defined length. [ISO/IEC WD 18033-1 (12/2001)]	42
Block Cipher	Symmetric encryption algorithm with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. [ISO/IEC 18033-1]	41
Block Cipher	Symmetric encryption algorithm with the property that the encryption process operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. [ISO/IEC 18033-1 (02/2001)]	42

Term	Definition	Source
Business Network	An entity’s communication network, used for general purpose business activities, typically connecting a wide variety of non-critical assets and non-safety related business applications.	38, 39
Certificate	See “public key certificate.”	10
Certificate	1. In cryptography, the public key and the identity of an entity, with other information, rendered unforgeable by digitally signing the entire information with the private key of the issuing certification authority. [After X9.42] Synonym digital certificate. 2. [A] record holding security information about an information-system (IS) user and vouches to the truth and accuracy of the information it contains. [INFOSEC-99] [ATIS]	41
Certificate	An entity’s data rendered unforgeable with the private or secret key of a certification autority. [ISO/IEC WD 13888-1 (11/2001)] A declaration by an independent authority operating in accordance with ISO Guide 58, Calibration and testing laboratory accreditation systems – General requirements for operation and recognition, confirming that an evaluation pass statement is valid. [ISO/IEC 15292: 2001]	42
Certificate	An encrypted file containing user or server identification information, which is used to verify identity and to help establish a security-enhanced link.	43
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	14, 15
Certification	[The] comprehensive evaluation of the technical and nontechnical security features of an AIS [automated information system] and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. [NIS] [FS-1037C]	41
Certification	Procedure by which a third party gives written assurance that a deliverable (product, system or service) conforms to specified requirements. [ISO/IEC WD 15443-1 (11/2001)]	42
Certification Authority (CA)	1. An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users‘ keys. [ISO/IEC 13888-1: 2004-06-01] 2. In cryptography, a centre trusted by one or more agencies or individuals to create and assign certificates and, optionally, to create user’s keys. [After X9.31] 3. In secure communications, a trusted person or entity who issues certificates (also called “public-key certificates”) for encryption	41

Term	Definition	Source
	purposes. 4. An independent party identifying and certifying payers and payees for real-time credit card transactions in electronic commerce. [Mattila] 5. Third level of the Public Key Infrastructure (PKI) Certification Management Authority responsible for issuing and revoking user certificates, and exacting compliance to the PKI policy as defined by-the parent Policy Creation Authority (PCA). [INFOSEC-99] [ATIS] 6. The entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates, and exacting compliance to a PKI policy. [RFC2828]	
Certification Authority (CA)	A centre trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities. [ISO/IEC 9796-3: 2000, ISO/IEC 11770-1: 1996, ISO/IEC 11770-3: 1999]	42
Cipher	1. Cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys [ISO/IEC 18033-1] 2. A cipher is any cryptographic system in which arbitrary symbols, or groups of symbols, represent units of plain text of regular length, usually single letters, or in which units of plain text are rearranged, or both, in accordance with certain predetermined rules. 2. The result of using a cipher. *Note:* An example of a cipher is an enciphered or text. [FS-1037C]	41
Cipher	Alternative term for encryption algorithm. [ISO/IEC WD 18033-1 (12/2001)]	42
Cipher	The method used to transform a readable message (called plaintext or cleartext) into an unreadable, scrambled or hidden message (called ciphertext).	43
Cipher Text	Enciphered information. [ISO 8372: 1987]	42
Ciphertext	Data in its encrypted form.	10
Ciphertext	Data which has been transformed to hide its information content [ISO/IEC 10116:1997]	41
Ciphertext	Data which has been transformed to hide its information content. [ISO/IEC 9791-1: 1999, ISO/IEC 9798-1: 1997, ISO/IEC CD 10116 (12/2001), ISO/IEC WD 18033-1 (12/2001)]	42
Ciphertext	Data that has been encrypted. Ciphertext is the output of the encryption process and can be transformed back into a readable form plaintext with the appropriate decryption key.	43
Cleartext	Unencrypted data without format additions or changes, such as	10

Term	Definition	Source
	framing or padding.	
Cleartext	*Synonym*: *Plaintext*. Unencrypted information. [INFOSEC-99] [FS-1037C]	41
Cleartext	Alternative term for plaintext. [ISO/IEC WD 18033-1 (12/2001)]	42
Cleartext	See plaintext.	43
Client	A device or program requesting a service.	10
Client	A device or application receiving or requesting services or information from a server application. [ATIS]	41
Common Security Control	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.	15
Common Security Control	Security controls that can be applied to one or more organizational information systems and have the following properties: (i) the development, implementation, and assessment of the controls can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the controls can be used to support the security certification and accreditation processes of organizational information systems where those controls have been applied.	14
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.	15
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization under strict terms and conditions in lieu of the prescribed security controls in the low, moderate, or high security control baselines, that provide equivalent or comparable protection for an information system.	14
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices.	1, 10, 12
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	14, 15, 18

Term	Definition	Source
Confidentiality	1. Of classified or sensitive data, the degree to which the data have not been compromised; i.e., have not been made available or disclosed to unauthorized individuals, processes, or other entities. [After 2382-pt.8] 2. Assurance that information is not disclosed to unauthorized persons, processes, or devices. [INFOSEC-99] 3. A property by which information relating to an entity or party is not made available or disclosed to unauthorized individuals, entities, or processes. [T1.Rpt22-1993] [ATIS] 4. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST] 5. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 7498-2]	41
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Control System	Those facilities, systems, and equipment that comprise the operational real-time control environment, services, diagnostics, and functional capabilities necessary for the effective and reliable operation of the bulk electric system.	38, 39
Control System	A control system is a device or set of devices that manage the behaviour of other devices. Some devices or systems are not controllable. A control system is an interconnection of components connected or related in such a manner as to command, direct, or regulate itself or another system. There are two common types of controllers, with many variations and combinations: logic controls, and feedback or linear controls. There is also fuzzy logic, which attempts to combine the easy design of logic with the real-world utility of feedback controls. [WIKI]	41
Counter (CTR)	An encryption mode, in which a set of input blocks, called counters, is fed to the cipher to produce a sequence of output blocks that are XORed with the plaintext to produce the ciphertext.	10
Counter	1. A device or register in a digital processor for determining and displaying the total number of occurrences of a specific event. 2. In the opposite direction. 3. Device or PC program element that can total binary events and perform ON/OFF actions based on the value of the total. 4. A device, register, or location in storage for storing numbers or number representations in a manner which permits these numbers to be increased or decreased by the value of another number, or to be changed or reset to zero or to an arbitrary value.	33
Counter	A bit array of length *n* bits which is used in the Counter Mode; its value when considered as the binary representation of an integer increases by one (modulo 2<SUPn) after each block of plaintext is processed	42

Term	Definition	Source
	[ISO/IEC CD 10116 (12/2001)]	
Countermeasure	An action taken in opposition to a threat, or to reduce or eliminate vulnerabilities. They may be safeguards or secureguards.	32
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.	12, 14, 15
Critical Asset	Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.	36
Critical Assets	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailalble, would affect the reliability or operability of the Bulk Electric System	35
Critical Assets	Those facilities, systems, and equipment, which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the bulk electric system, or would cause significant risk to public health and safety.	38, 39
Critical Cyber Assets	Cyber Assets essential to the reliable operation of Critical Assets.	35
Critical Cyber Assets	Those cyber assets essential to the reliable operation of critical assets.	39
Cryptographic Key (key)	A parameter used in conjunction with a cryptographic algorithm that defines the transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, a digital signature computed from data, the verification of a digital signature computed from data, an authentication code computed from data, or an exchange agreement of a shared secret.	1, 10
Cryptographic key	A mathematical value that is used (a) in an algorithm to generate cipher text from plain text or vice versa, and (b) to determine the operation of a cryptographic function (e.g., the synchronized generation of keying material), or a digital signature computation or validation. [After X9.31] [ATIS]	41
Cryptographic Module (CM)	The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.	10
Cryptographic	The set of hardware, software, and/or firmware that implements	1

Term	**Definition**	**Source**
Module	approved security functions (including cryptographic algorithms and key generation) and are contained within the cryptographic boundary.	
Cryptography	The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.	7, 10
Cryptography	1. [The] art or science concerning the principles, means, and methods for rendering plain information unintelligible, and for restoring encrypted information to intelligible form. [INFOSEC-99] 2. The branch of cryptology that treats of the principles, means, and methods of designing and using cryptosystems. [ATIS] 3. The discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [ISO/IEC 2nd WD 18014-2: 2006-04-04]	41
Cryptography	The study or analysis of codes and encoding methods used to secure information. Cryptographic techniques can be used to enable and ensure confidentiality, data integrity, authentication (entity and data origin), and nonrepudiation.	43
Cyber	Of, relating to, or involving computers or computer networks.	32
Cyber	*Loosely,* a prefix referring to anything related to computers or networking. *Note 1:* For example, a “cyber I” is a coffee shop that offers computer terminals for customers to browse the Internet while sipping coffee, and a “cyber sleuth” is an investigator who researches and attempts to solve or find the cause of, unusual Internet occurrences. *Note 2:* While “cyber” is listed herein as colloquial, its use has become ubiquitous and it is rapidly becoming accepted as formal language. [ATIS]	41
Cyber Attack	Exploitation of the software vulnerabilities of information technology-based control components.	10
Cyber Attack	*See Attack*	41
Cyber Security	*Synonym: Information Security.* The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. [ATIS]	41
Cybersecurity	The protection of digital systems and their support systems from threats of: • Cyberspace attack by adversaries who wish to disable or manipulate them. • Physical attack by adversaries who wish to disable or manipulate them. Access by adversaries who want to obtain, corrupt, damage or destroy sensitive information. This is an aspect of information security.	32

Term	Definition	Source
	Electronic data can be obtained by theft of computer storage media or by hacking into the computer system. Note that a cyberspace attack may be mounted to obtain sensitive information to plan a future physical or cyberspace attack.	
Data	1. Information of any type. 2. A common term used to indicate the basic elements that can be processed or produced by a computer.	33
Data Integrity	1. [The] condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [NIS] 2. The condition in which data are identically maintained during any operation, such as transfer, storage, and retrieval. [FIPS 140-2]88) 3. The preservation of data for their intended use. 4. Relative to specified operations, the a priori expectation of data quality. [FS-1037C]	41
Data Integrity	The property that data has not been altered or destroyed in an unauthorized manner. [ISO/IEC 9797-1; 1999]	42
Decryption	The process of changing ciphertext into plaintext using a cryptographic algorithm and key.	10
Decryption	1. Reversal of a corresponding encryption. [ISO/IEC 18033-1] 2. The process of changing ciphertext into plaintext using a cryptographic algorithm and key. [RFC2828]	41
Decryption	Reversal of a corresponding encipherment. [ISO/IEC WD 18033-1 (12/2001)]	42
Demilitarized Zone	Perimeter network segment that is logically between internal and external networks. It purpose is to enforce the internal network’s policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.	12
Demilitarized Zone	DMZ is a term used in complex firewall configurations, where a device is placed outside the firewall, but is still available for use by the internal (protected) network.	13
Denial-of-Service (DOS)	The prevention of authorized access to a system resource or the delaying of system operations and functions. (See “interruption.”)	10
Denial-of-Service (DOS)	1. The prevention of authorized access to resources or the delaying of time-critical operations. [2382-pt.8] 2. The result of any action or series of actions that prevents any part of an information system (IS) from functioning. [INFOSEC-99] [ATIS] 3. The prevention of authorized access to a system resource or the delaying of system operations and functions. (*See*: *availability, critical (resource of a system), flooding.*) [RFC2828]	41

Term	Definition	Source
Digital Signature	The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation.	1, 10
Digital Signature	1. Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO/IEC 13888-1: 2004-06-01] 2. A cryptographic modification of data that provides: (a) origin authentication, (b) data integrity, and (c) signer non-repudiation (when associated with a data unit and accompanied by the corresponding public-key certificate). [After X9.49] A cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. Synonym electronic signature. [INFOSEC-99] [ATIS] 3. The result of a cryptographic transformation of data which, when properly implemented, provides the services of: • origin authentication• data integrity• signer non-repudiation. [FIPS 140-2]	41
Digital Signature	A data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient. [ISO/IEC 11770-3: 1999] Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery, e.g. by the recipient. [ISO/IEC FDIS 15946-3 (02/2001)] A cryptographic transformation of a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient. NOTE - Digital signatures may be used by end entities (see below) for the purposes of authentication, of data integrity, and of non-repudiation of creation of data. The usage for non repudiation of creation of data is the most important one for legally binding digital signatures. [ISO/IEC 15945: 2002]	42
Digital Signature	Data that binds a sender's identity to the information being sent. A digital signature may be bundled with any message, file, or other digitally encoded information, or transmitted separately. Digital signatures are used in public key environments and provide nonrepudiation and integrity services.	43
Digital Signature (Signature)	Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery, e.g. by the recipient. [ISO/IEC 9798-1: 1997]	42
Distributed Control Systems (DCS)	A DCS is a type of plant automation system similar to a SCADA system, except that a DCS is usually employed in factories and is	32

Term	Definition	Source
	located within a more confined area. It uses a high-speed communications medium, which is usually a separate wire (network) from the plant LAN. A significant amount of a closed loop control is present in the system	
Distributed Control Systems (DCS)	In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit.	33
Electronic Security Perimeter	The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.	35, 39
Element	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components.	34
Element	An indivisible security requirement. [ISO/IEC 15408-1: 1999]	42
Emulate	To represent a system by a model that accepts the same inputs and produces the same outputs as the system represented. For example, to emulate an 8-bit computer with a 32-bit computer.	10
Emulate	To imitate one system with another such that the imitating system accepts the same data, executes the same programs, and achieves the same results as the imitated system.	33
Encryption	Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state. [RFC 2828]	10
Encryption	1. (Reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data. [ISO/IEC 18033-1] 2. The process of changing plaintext into ciphertext using a cryptographic algorithm and key. [RFC2828]	41
Encryption	(Reversible) transformation of data by a cryptographic algorithm to produce ciphertext, I.e. to hide the information content of the data. [ISO/IEC WD 18033-1 (12/2001)]	42
Encryption	The process of converting data into a coded form (ciphertext) to prevent it from being read and understood by an unauthorized party.	43
Entity	An individual, organization, device or process.	10

Term	Definition	Source
Entity	An active element within an OSI layer (e.g. Token Bus MAC is an entity in the Layer 2). [Editor’s note: ISA definition of OSI: Abbreviation for open system interconnection (a connection between one communication system and another using a standard protocol).]	33
Entity	The facility or critical asset owner, operator, etc.	36
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.	12, 14
Environment	The ambient natural and artificial conditions that surround a piece of operating equipment.	33
Extranet	An extranet can be viewed as a part of a company’s intranet that is extended to users outside the company. It has also been described as a “state of mind,” in which the Internet is perceived as a way to do business with other companies as well as to sell products to customers.	13
Extranet	An extension of an organization's intranet used to facilitate communication with the organization's trusted partners. An extranet allows such trusted partners to gain limited access to the organization's internal business data.	43
Firewall	System designed to defend against unauthorized access to or from a private network. [CNSS]	12
Firewall	A set of programs residing on a gateway server that protect the resources of an internal network. Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall is often installed in a specially designated computer that is separate from the rest of the network so that no incoming request can get directly at private network resources. There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain name and Internet Protocol addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates.	13

Term	Definition	Source
Firewall	A security solution which segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic filtering rules.	43
Firmware	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.	1, 10
Firmware	Programs or instructions that are permanently stored in hardware memory devices (usually read-only memories) that control hardware at a primitive level.	33
Hardware	The physical equipment within the cryptographic boundary used to process programs and data.	1, 10
Hardware	1. Physical equipment directly involved in performing industrial process measuring and controlling functions. 2. In data processing, hardware refers to the physical equipment associated with the computer.	33
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: It is computationally infeasible to find any input that map to any pre-specified output, and It is computationally infeasible to find any two distinct inputs that map to the same output.	10
Hash Function	1. A function which maps strings of bits to fixed-length strings of bits,	41

Term	Definition	Source
	satisfying two properties. - it is computationally infeasible to find for a given output, an input which maps to this output; - it is computationally infeasible to find for a given input, a second input which maps to the same output. NOTES a – The literature on this subject contains a variety of terms which have the same or similar meaning as hash-function. Compressed encoding and condensing function are some examples. b – Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC PreFDIS 9796-3: 2006-01-26] 2. A computational function performed on a message with results similar to a cyclic redundancy check. A good cryptographic hash function has the following characteristics: a) Any change to the message is likely to affect the hashed value; b) It is computationally infeasible to derive the original message from the hashed value; c) It is computationally infeasible to find another message that produces the same hashed value. [WIKI]	
Hash-function	A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties. It is computationally infeasible to find for a given output, an input which maps to this output. It is computationally infeasible to find for a given input, a second input which maps to the same output. NOTE - Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1: 2000] A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties. For a given output, it is computationally infeasible to find an input which maps to this output; For a given input, it is computationally infeasible to find a second input which maps to the same output. NOTE - Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC 14888-1: 1998] Function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties. It is computationally infeasible to find for a given output an input which maps to this output. It is computationally infeasible to find for a given input a second input which	42

Term	Definition	Source
	maps to the same output. [ISO/IEC 9798-5: 1999] A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: For a given output, it is computationally infeasible to find an input which maps to this output; and For a given input, it is computationally infeasible to find a second input which maps to the same output. NOTE - Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 9796-3: 2000, ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)] Function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties. For a given output, it is computationally infeasible to find an input which maps to this output. For a given input, it is computationally infeasible to find a second input which maps to the same output. [ISO/IEC FDIS 9796-2 (12/2001); ISO/IEC FDIS 9797-2 (09/2000)] A function which maps strings of bits to fixed-length strings of bits, satisfying two properties. It is computationally infeasible to find for a given output, an input which maps to this output. It is computationally infeasible to find for a given input, a second input which maps to the same output. The literature on this subject contains a variety of terms which have the same or similar meaning as hash-function. Compressed encoding and condensing function are some examples. Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC FDIS 15946-3 (02/2001)]	
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	14, 15, 18
Information Security	The protection of written, verbal and electronic information against unauthorized disclosure, transfer, modification, or destruction. Traditionally, information technology security has focused on the confidentiality, integrity and availability of data.	32

Term	Definition	Source
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [NIST]	41
Information Security	The preservation of confidentiality, integrity and availability of information. NOTE - Confidentiality is defined as ensuring that information is accessible only to those authorized to have access. Integrity is defined as safeguarding the accuracy and completeness of information and processing methods. Availability is defined as ensuring that authorised users have access to information and associated assets when required. [ISO/IEC 17799: 2000]	42
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.	1, 10
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	14, 15, 18
Integrity	Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.	12
Integrity	1. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [NIST] 2. The property that sensitive data have not been modified or deleted in an unauthorized and undetected manner. [FIPS 140-2] 3. Property that sensitive data has not been modified or deleted in an unauthorised and undetected manner. [ISO/IEC 19790: 2006-03-01]	41
Integrity	The property of safeguarding the accuracy and completeness of assets. [ISO/IEC PDTR 13335-1 (11/2001)]	42

Term	Definition	Source
Interface	A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals. [FIPS 140-2]	1, 10, 41
Interface	A specific electronic circuit that is a boundary between other circuits or devices.	33
Internal	Information that is accessible to all Employees and Contractors while providing services to the operator. For Operators use only (See Information Distribution for more details.)	13
Internal	In PC ladder programs, a coil or contact whose reference is a logical element in the program and not directly concerned with I/O. May also refer to the storage location used for the logical status of such an element. [Editor's note: ISA defines I/O as Acronym for Input/Output.]	33
Intrusion	Unauthorized act of bypassing the security mechanisms of a system.	12
Intrusion	A deliberate or accidental set of events that potentially causes unauthorized access to, activity against, and/or activity in, an information technology (IT) system. [ISO/IEC DTR 15947 (10/2001)]	42

Term	Definition	Source
Intrusion Detection System (IDS)	Information system used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in Information Systems and networks. [ISO/IEC FDIS 18043: 2006-03-14]	41
Intrusion Detection System (IDS)	A technical system that is used to identify and respond to intrusions in IT systems. [ISO/IEC DTR 15947 (10/2001)]	42
Key [alpha order: put all words beginning with "key" together, alphabetized according to second word]	See cryptographic key	10
Key	1. Sequence of symbols that controls the operation of a cryptographic transformation (e.g. encryption, decryption). [ISO/IEC 18033-1] 2. Unique digital information used to perform a cryptographic operation such as hashing, encryption or decryption. Called a key because it serves a similar purpose as a physical key in that the key is required to "lock" or "unlock" encrypted or hashed information. [WIKI]	41
Key	A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification). [ISO/IEC 9797-1: 1999, ISO/IEC 9798-1: 1997, ISO/IEC 11770-1: 1996] A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature calculation, or signature verification). [ISO/IEC 11770-3: 1999] A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment). [ISO/IEC CD 10116 (12/2001)] A sequence of symbols that controls the operation of a cryptographic transformation (e.g.encipherment, decipherment, cryptographic check function computation, signature generation, signature verification, or key agreement). [ISO/IEC FDIS 15946-3 (02/2001)]	42

Term	**Definition**	**Source**
	Sequence of symbols that controls the operation of a cryptographic transformation (e.g.encipherment, decipherment). [ISO/IEC WD 18033-1 (12/2001)]	
Key	In encryption and digital signatures, a value used in combination with an algorithm to encrypt or decrypt data.	43
Key Confirmation	A process used to validate the accuracy and authenticity of a parameter used in the encryption or decryption function.	10
Key Confirmation	The assurance for one entity that another identified entity is in possession of the correct key. [ISO/IEC 11770-1: 1996, ISO/IEC 11770-2: 1996]	42
Key Establishment	The process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).	1
Key establishment	The process by which cryptographic keys are distributed securely among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement). [1]	10

Term	Definition	Source
Key Establishment	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.	1, 10
Key Management	The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy. [ISO/IEC 11770-1: 1996]	42
Key Pair	A public key and its corresponding private key. A key pair is used with a public key algorithm.	10
Key Pair	A public key and its corresponding private key used with a public key algorithm. [RFC2828]	41
Keying Material	A string of numbers and/or characters, identically having a high degree of randomness or unpredictability, used to carry out an agreed upon logical function.	10
Keying Material	The data (e.g. keys, initialisation values) necessary to establish and maintain cryptographic keying relationships. [ISO/IEC 11770-1: 1996]	42
Latency	The time it takes for a packet to cross a network connection, from sender to receiver.	10

Term	Definition	Source
Latency	In data processing, the time between the completion of the interpretation of an address and the start of the actual transfer from the addressed location. Latency includes the delay associated with access to storage devices such as drums and delay lines.	33
Latency	Time delay between the moment something is initiated, and the moment one of its effects begins. [WIKI]	41
Local Area Network (LAN	A communications network designed to connect computers and other intelligent devices in a limited geographic area (typically under 10 km. [ATIS]	41
Local Area Networks	Acronym for local area network, a group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.	13
Masquerade	The pretence by an entity to be a different entity in order to gain unauthorized access. [ATIS]	41
Masquerade	The pretence by an entity to be a different entity. [ISO/IEC 9798-1: 1997]	42
Master	A device that initiates communications requests to gather data or perform controls.	2, 10
Master	1. A device which controls other devices in a system. 2. A precise pattern for making replicate workpieces, as in certain types of casting processes.	33
Media	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.	14
Media	1. The physical interconnection between devices attached to the LAN. Typical LAN media are twisted pair, baseband coax, broadband coax, and fiber optics. 2. The plural of medium.	33
Message	An ordered series of characters used to convey information.	10
Message	An arbitrary amount of information whose beginning and end are defined or implied.	33

Term	Definition	Source
Message	String of bits of any length. [ISO/IEC FDIS 9796-2 (12/2001)] A string of bits of any length. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998, ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)	42
Message Authentication Code (MAC)	Data that is associated with authenticated information that allows an entity to verify the integrity of the information.	10
Message Authentication Code (MAC)	The string of bits which is the output of a MAC algorithm. NOTE – A MAC is sometimes called a cryptographic check value. [ISO/IEC 9797-1: 1999, ISO/IEC WD 13888-1 (11/2001)]	42
Message Authentication Code (MAC)	An algorithm that allows a receiver to ensure that a block of data has retained its integrity from the time it was sent until the time it was received.	43
Multicast	A message addressed to a group of stations connected to a LAN.	33
Multicast	1. In a network, a technique that allows data, including packet form, to be simultaneously transmitted to a selected set of destinations. Note: Some networks, such as Ethernet, support multicast by allowing a network interface to belong to one or more multicast groups. 2. To transmit identical data simultaneously to a selected set of destinations in a network, usually without obtaining acknowledgement of receipt of the transmission. [ATIS]	41
Non-Repudiation	A service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the originator.	10
Non-Repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.	12, 15
Non-Repudiation	1. The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later [ISO/IEC 13888-1; ISO IS 7498-2] 2. A security service that provides protection against false denial of involvement in a communication. [RFC2828]	41
Non-repudiation	The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later. [ISO/IEC PDTR 13335-1 (11/2001)]	42

Term	Definition	Source
Nonrepudiation	A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Nonrepudiation provides undeniable proof that a user took a specific action such as transferring money, authorizing a purchase, or sending a message.	43
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.	1, 10
Password	1. Secret word, phrase, number or character sequence used for entity authentication, which is a memorized weak secret. [ISO/IEC FDIS 11770-4: 2006-01-09] 2. A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. [FIPS 140-2]	41
Password	A string of characters entered by a user to verify his or her identity to a network or to a local computer. See also strong password and weak password.	43
Personal Identification Number (PIN)	An alphanumeric code or password used to authenticate an identity. [FIPS 140-2]	41
Personal Identification Number (PIN)	A secret identification code similar to a password that is assigned to an authorized user. A PIN is used in combination with an ATM card or smart card, for example, to unlock an authorized functionality such as access to a bank account.	43
Physical Security Perimeter	The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.	35
Physical Security Perimeter	A type of gate, door, wall, or fence system that is intended to restrict and control the physical access or egress of personnel.	36
Physical Security Perimeter	The physical border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which critical cyber assets are housed and for which access is controlled.	39
PKI [See public Key Infrastructure]	Public Key Infrastructure	41
PKI	See public key infrastructure.	43
Plaintext	Unencrypted data with format additions or changes, such as framing or padding.	10
Plaintext	Unencrypted information. [ISO/IEC 10116: 2006-02-01]	41

Term	Definition	Source
Plaintext	Unenciphered information. [ISO 8372: 1987, ISO/IEC 9797-1: 1999, ISO/IEC 9798-1: 1997, ISO/IEC CD 10116 (12/2001), ISO/IEC WD 18033-1 (12/2001)]	42
Plaintext	Data in its unencrypted or decrypted form.	43
Port	A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).	1, 10
Port	1. The entry or exit point from a computer for connecting communications or peripheral devices. 2. An aperture for passage of steam or other fluids.	33
Principal	An entity whose identity can be authenticated. [ISO/IEC 9798-1: 1997]	42
Principal	See security principal.	43
Private Key	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.	1, 10
Private Key	1. That key of an entity's asymmetric key pair which should only be used by that entity. [ISO/IEC 11770-1: 1996] 2. One of a pair of keys used to perform asymmetric encryption in public key cryptography. The private key is kept secret, while the public key may be widely distributed. In a sense, one key "locks" a lock; while the other is required to unlock it. It should not be feasible to deduce the private key of a pair given the public key, and in high quality algorithms no such technique is known. [WIKI]	41
Private Key	That key of an entity's asymmetric key pair which should only be used by that entity. NOTE - A private key shall not normally be disclosed. [ISO/IEC 11770-1: 1996, ISO/IEC WD 18033-1 (12/2001)] That key of an entity's asymmetric key pair which should only be used by that entity. NOTE - In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation. [ISO/IEC 9798-1: 1997, ISO/IEC FDIS 15946-3 (02/2001)] That key of an entity's asymmetric key pair which can only be used by that entity. NOTE - In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation. [ISO/IEC 11770-3: 1999, ISO/IEC WD 13888-1	42

Term	Definition	Source
	(11/2001)] That key of an entity's asymmetric key pair which should only be used by that entity. [ISO/IEC FDIS 9796-2 (12/2001)]	
Private Key	One of two keys in public key encryption. The user keeps the private key secret and typically uses it to digitally sign data, or to decrypt data that has been encrypted with the corresponding public key.	43
Programmable Logic Controller (PLC)	A PLC is a hardened, special-purpose computer that was developed to replace relay-based control systems. PLCS are often integrated with DCSs to obtain the benefit of a superior user interface by the DCS consoles. PCs are being used to replace PLCs in some applications since the offer standard hardware, software, and graphical user interfaces.	32
Programmable Logic Controller (PLC)	Abbreviation for programmable logic controller, microcomputer-based control device used to replace relay logic.	33
Protection Profile	An implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs. [FIPS 140-2]	41
Protection Profile	An implementation-independent set of security requirements for a category of IT products or systems that meet specific consumer needs. [ISO/IEC 15292: 2001] An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs. [ISO/IEC 15408-1: 1999]	42
Public Key	A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. (Public keys are not considered CSPs.)	1, 10
Public Key	1. That key of an entity's asymmetric key pair which can be made public. [ISO/IEC 9798-1: 1997] 2. A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. [FIPS 140-2]	41
Public Key	That key of an entity's asymmetric key pair which can be made public. [ISO/IEC FDIS 9796-2 (12/2001), ISO/IEC 11770-1: 1996, ISO/IEC WD 18033-1 (12/2001)] That key of an entity's asymmetric key pair which can be made public. NOTE - In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-	42

Term	Definition	Source
	specified group. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-3: 1999, ISO/IEC WD 13888-1 (11/2001), ISO/IEC FDIS 15946-3 (02/2001)]	
Public Key	One of two keys in public key encryption. The user releases this key to the public, who can use it to encrypt messages to be sent to the user and to verify the user's digital signature. Compare with private key.	43
Public key (asymmetric) cryptographic algorithm	A cryptographic algorithm that uses two related keys — a public key and a private key. The two keys have the property that deriving the private key from the public key is not computationally feasible. [1]	1, 10
Public Key Asymmetric Cryptographic Algorithm	A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. [FIPS 140-2]	41
Public Key Certificate	A set of data that uniquely identifies an entity, contains the entity’s public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. [FIPS 140-2]	1, 10, 41
Public Key Certificate	The public key information of an entity signed by the certification authority and thereby rendered unforgeable. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-1: 1996, ISO/IEC 11770-3: 1999, ISO/IEC WD 13888-1 (11/2001)] The public key information of an entity signed by the certification authority and thereby rendered unforgeable. NOTE - In the context of this part of ISO/IEC 9796 the public key information contains the information about the verification key and the domain parameters. [ISO/IEC 9796-3: 2000]	42
Public Key Infrastructure (PKI)	A framework that is established to issue, maintain and revoke public key certificates. [RFC2828]	10, 41
Public Key Infrastructure (PKI)	The system consisting of TTPs, together with the services they make available to support the application (including generation and validation) of digital signatures, and of the persons or technical components, who use these services. NOTE - Sometimes the persons and the technical components participating in a PKI by using the services of TTPs, but not being TTPs themselves, are referred as end entities. An example of a technical equipment used by an end entity is a smart card which may be used as a storage and or processing device. [ISO/IEC 15945: 2002]	42
Public Key Infrastructure (PKI)	A framework encompassing the laws, policies, standards, hardware, and software to provide and manage the use of public key cryptography on public networks such as the Internet.	43

Term	Definition	Source
Remote Access	Access by users (or information systems) communicating external to an information system security perimeter.	15
Remote Access	Pertaining to communication with a data processing facility by one or more stations that are distant from that facility.	33
Replay Attack	1. A masquerade which involves use of previously transmitted messages. [ISO/IEC 9798-1: 1997-08-01] 2. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack. [WIKI]	41
Replay Attack	A masquerade which involves use of previously transmitted messages. [ISO/IEC 9798-1: 1997]	42
Repudiation	The ability to deny that a transaction took place (for example an individual could claim “I never performed that action”).	3, 10
Repudiation	The ability to deny that a transaction took place (e.g., “I never performed that control.” [RFC2828]	41
Repudiation	The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.	43
Residual Risk	The remaining risk after the security controls have been applied.	12
Residual Risk	The risk that remains after implementation of the IT security plan. [ISO/IEC PDTR 13335-1 (11/2001)] Any combination of the risk that have been accepted by the organization, the risks that remain after all identified controls have been implemented because further action could not be identified. [ISO/IEC 17799; 2000]	42
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [FIPS PUB 200 (2005)]	10
Risk	Possibility that a particular threat will adversely impact a system by exploiting a particular vulnerability.	12
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals results from the operation of an information system given the potential impact of a	14, 15, 30

Term	Definition	Source
	threat and the likelihood of that threat occurring.	
Risk	1. The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence. [ISO/IEC 13335-1: 2004-11-15] 2. An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. [RFC2828]	41
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Risk Analysis	The process of estimating risks.	32
Risk Analysis	The systematic process of estimating the magnitude of risks. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.	15, 30
Risk Assessment	The process of using risk analysis results to make decisions on risk reduction.	32
Risk Assessment	1. A risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The target of the risk assessment process is the identification and evaluation of risks, which have negative impacts to identified assets and the definition of appropriate safeguards and actions, which minimize the effects of the identified risks. [ISO/IEC 5th WD 15443-3:2005-06-03] 2. Risk assessment is a step in the risk management process. Risk assessment is measuring two quantities of the risk, the magnitude of the potential loss, and the probability that the loss will occur. Risk assessment may be the most important step in the risk management process, and may also be the most difficult and prone to error. Once risks have been identified and assessed, the steps to properly deal with them are much more programmatical. [WIKI]	41

Term	Definition	Source
Risk Assessment	The process of combining risk identification, risk analysis and risk evaluation. [ISO/IEC PDTR 13335-1 (11/2001)] The assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence. [ISO/IEC 17799: 2000]	42
Risk Management	Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.	12, 30
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.	15
Risk Management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.	14
Risk Management	The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost	32
Risk Management	The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect IT system resources. [ISO/IEC PDTR 13335-1 (11/2001)] The process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost. [ISO/IEC 17799: 2000]	42
Role	A set of transactions that a user or set of users can perform within the context of an organization.	10
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE. [ISO/IEC 15408-1: 1999]	42
RSA	The public key algorithm invented by Rivest, Shamir, and Adleman.	10
RSA	RSA (Rivest, Shamir and Adleman) is an algorithm for public-key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is still widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys. [WIKI]	41

Term	Definition	Source
Safeguard	A practice, procedure or mechanism that reduces risk. Note that the term ‘safeguard’ is normally considered to be synonymous with the term ‘control’. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Safeguard	A technology, policy, or procedure that counters a threat or protects assets.	43
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.	12*, 14, 15
SCADA [See also Supervisory Control and Data Acquisition below.]	See “supervisory control and data acquisition system.”	10
SCADA [See also Supervisory Control and Data Acquisition below.]	Abbreviation for supervisory control and data acquisition technique (in industrial control/monitor work).	33
SCADA [See also Supervisory Control and Data Acquision below.]	Supervisory Control and Data Acquisition. The term refers to a large-scale, distributed measurement and control system. The three components of a SCADA system are: • Multiple Remote Terminal Units (also known as RTUs). • Central Control Room with Host Computer(s). Communication infrastructure. [WIKI]	41
Scoping Guidance	Provides organizations with specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security controls in the control baseline.	15
Scoping Guidance	Specific factors related to technology, infrastructure, public access, scalability, common security controls, and risk that can be considered by organizations in the applicability and implementation of individual security controls in the security control baseline.	14
Secret Key	A cryptographic parameter that is held private by one or more entities to limit the ability to communicate or access that group or entity.	10
Secret Key	1. A key used with symmetric cryptographic techniques and usable only by a set of specified entities. [ISO/IEC 13888-1: 2004-06-01] 2. A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. [FIPS 140-2]	41

Term	Definition	Source
Secret Key	A key used with symmetric cryptographic techniques and usable only by a set of specified entities. [ISO/IEC 11770-1: 1996, ISO/IEC WD 13888-1 (11/2001)] A key used with symmetric cryptographic techniques by a set of specified entities. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)] Key used with symmetric cryptographic techniques by a set of specified entities. [ISO/IEC WD 18033-1 (12/2001)]	42
Secure Shell	A set of commands and protocols that uses digital certificates for authenticating host and client as well as for encrypting communications to ensure security.	13
Secure Shell (SSH)	A protocol that provides secure remote login utilising an insecure network. SSH is proprietary but will become an IETF standard in the near future. SSH was originally developed by SSH Communications Security. [ISO/IEC 18028-4: 2005-04-01]	41
Security	Protection against threats and attacks.	32
Security	1. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. [JP1] 2. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. [After JP1] 3. Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. [JP1] [ATIS] 4. All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability. [ISO/IEC 13335-1]	41
Security	All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability. NOTE - A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way. This is usually considered in the context of an assessment of actual or perceived threats. [ISO/IEC WD 15443-1 (11/2001)]	42
Security	See computer security.	43

Term	Definition	Source
Security Domain	A system or subsystem that is under the authority of a single trusted authority. Security domains may be organized (e.g., hierarchically) to form larger domains. [RFC2828]	10, 41
Security Domain	A collections of users and systems subject to a common security policy. [ISO/IEC 15816: 2002]	42
Security Objective	Confidentiality, integrity, or availability.	14, 15, 25
Security Objective	A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions. [ISO/IEC 15408-1; 1999]	42
Security Performance	Security performance may be evaluated in terms of a program's compliance, completeness of measures to provide specific threat protection, post compromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure that security measures remain effective and appropriate. Tests, audits, tools, measures, or other methods are required to evaluate security practice performance.	11
Security Performance	Security Performance—Security performance may be evaluated in terms of a program's compliance, completeness of measures to provide specific threat protection, post compromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure that security measures remain effective and appropriate. Tests, audits, tools, measures, or other methods are required to evaluate security practice performance. [ISA SP99]	41
Security Plan	A document that describes an operator's plan to address security issues and related events, such as security assessments and mitigation options, and includes security levels and response measures to security threats.	13
Security Plan	See System Security Plan.	14, 15
Security Policies	Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from company or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.	11
Security Policy	See Cryptographic module security policy.	10

Term	Definition	Source
Security Policy	1. Set rules internal to an organizational unit that regulate how this unit protects the management of its assets conform to specified organizational objectives within its legal and cultural context. [ISO/IEC 15408] 2. A security policy is a plan of action for tackling security issues, or a set of regulations for maintaining a certain level of security. It can span anything from the practices for securing a single computer, to building/premises security, to securing the existence of an entire nation-state. [WIKI]	41
Session	A period defined either by an amount of time, a number of messages, or a user-initiated change during which two CMs operate using specific parameters.	10
Session	Layer 5 of OSI. [ISA definition of OSI: Abbreviation for open system interconnection (a connection between one communication system and another using a standard protocol). OSI reference model, Layer 5 – Session: provides user-to-user connections.]	33
Shall	Equivalent to "is required to", and is used to indicate mandatory requirements, strictly to be followed in order to conform to the standard and from which no deviation is permitted.	10
Shall	The term “shall” is used in this standard to indicate those practices that are mandatory	13
Should	Equivalent to “is recommended that,” is used to indicate several possibilities recommended as particularly suitable, without mentioning or excluding other, that a certain course of action is preferred but not required, that (in the negative form) a certain course of action is deprecated but not prohibited.	10
Should	The term “should” is used in this standard to indicate: ● Those practices for which engineering judgment is required. ● Those practices which are preferred, but for which operators may determine that alternative practices are equally or more effective.	13
Slave	A device that gathers data or performs control operations in response to requests from the master, and sends response messages in return. A slave device may also generate unsolicited responses.	10
Slave	A mechanical or electronic device that is under the control of a another [sic] device.	33
Software	The programs and data components within the cryptographic boundary, usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution.	1, 10
Software	1. A set of programs, procedures, rules, and possibly associated documentation concerned with the operation of a computer system, for	33

Term	Definition	Source
	example, compilers, library routines, manuals, circuit diagrams. 2. Contrast with hardware. [ISA definition of hardware: 1. Physical equipment directly involved in performing industrial process measuring and controlling functions. 2. In data processing, hardware refers to the physical equipment associated with the computer.]	
Spoof	Pretending to be an authorized user.	3, 10
Spoof	Pretending to be an authorized user and performing an unauthorized action. [RFC2828]	41
Spoof	To make a transmission appear to come from a user other than the user who performed the action.	43
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.	15
Spyware	Spyware covers a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party. Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, however, spyware - by design - exploits infected computers for commercial gain. Typical tactics furthering this goal include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card numbers); monitoring of Web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites. [WIKI]	41
Spyware	Software that can display advertisements (such as pop-up ads), collect information about you, or change settings on your computer, generally without appropriately obtaining your consent.	43
SSL	Secure Sockets Layer. SSL provides endpoint authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated; mutual authentication requires public key infrastructure (or PKI) deployment to clients. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery. [WIKI]	41
SSL	See Secure Sockets Layer (SSL).	43
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs	15

Term	Definition	Source
	one or more specific functions.	
Subsystem	A portion of a larger system consisting of several components or process units which, together, have the characteristics of a system by themselves.	33
Supervisory Control and Data Acquisition (SCADA) system	A system operating with coded signals over communication channels so as to provide control of remote equipment (using typically one communication channel per remote station). The supervisory system may be combined with a data acquisition system, by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions.	10
Supervisory Control and Data Acquisition (SCADA)	A computer control system used in real time to monitor and control one or more remote facilities. The system collects data and/or sends control instructions, either automatically or by operators at other locations. SCADA is used to control facilities in industries such as telecommunications, water and waste control, energy, oil and gas refining, and transportation.	32
Supervisory Control and Data Acquisition (SCADA)	A system of remote control and telemetry used to monitor and control the transmission system.	34
System	1. An assembly of procedures, processes, methods, routines, or techniques united by some form of regulated interaction to form an organized whole. 2. The complex or hardware and software utilized to affect the control of a process. 3. An assemblage of equipment, machines, control devices, or a combination thereof, interconnected mechanically, hydraulically, pneumatically or electrically, and intended to act together to perform a predetermined function. 4. In data processing, any group of software and hardware that is connected to operate as a unit.	33
System	See Information System.	14, 15
System	A combination of generation, transmission, and distribution components.	34
System	A specific IT installation, with a particular purpose and operational environment. [ISO/IEC 15408-1: 1999, ISO/IEC WD 15443-1 (11/2001)]	42
Threat	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.	10, 11

Term	Definition	Source
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.	12*, 14
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	15
Threat	The possibility of injury, damage, destruction, or diversion of an asset or other hostile action towards an asset.	32
Threat	1. Capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or a program or system or cause those to harm others. [ISO/IEC 1st WD 21827: 2006-02-07] 2. Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability. [NIST]	41
Threat	A potential cause of an unwanted incident that may result in harm to a system or organization. [ISO/IEC PDTR 13335-1 (11/2001)] A potential cause of an unwanted incident that may result in harm to an IT system. [ISO/IEC DTR 15947 (10/2001)] A potential cause of an unwanted incident which may result in harm to a system or organization. [ISO/IEC 17799: 2000]	42
Throughput	The total capability of equipment to process or transmit data during a specified time period.	10
Throughput	The net rate at which data can be received by a device, manipulated as specified, and output to some other specified device.	33
Throughput	The maximum continuous traffic rate that a device can handle without dropping a single packet. [ATIS]	41
Time-stamping Authority	A trusted third party trusted to provide evidence which includes the time when the secure time stamp is generated. [ISO/IEC 11770-3: 1999]	42
Time-stamping Authority (TSA)	A trusted third party trusted to provide a time stamping service. [ISO/IEC FDIS 18014-1 (02/2002)]	42
Token	A message consisting of data fields relevant to a particular communication and which contains information that has been	42

Term	Definition	Source
	transformed using a cryptographic technique. [ISO/IEC 9798-1; 1997]	
Token	See access token.	43
Traffic Analysis	Listening to messages, and without understanding their content, inferring information from the fact that certain messages are always sent when certain real-life events happen (e.g., closing a breaker).	3, 10
Traffic Analysis	1. In a communications system, the analysis of traffic rates, volumes, densities, capacities, and patterns specifically for system performance improvement. [From Weik '89] 2. [The] study of communications characteristics external to the text. [NIS] 3. The analysis of the communications-electronic environment for use in the design, development, and operation of new communications systems. [From Weik '89] 4. In cryptology, the inference of information from observation and analysis of the presence, absence, amount, direction, and frequency of the traffic flow. [After 2382-pt. 8] 5. [The] Study of communications patterns. [INFOSEC-99] [ATIS]	41
Trojan Horse	1. An apparently harmless program containing malicious logic that allows the unauthorized collection, falsification, or destruction of data. [2382-pt.8] 2. [A] program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. [INFOSEC-99]	41
Trojan Horse	A program that appears to be useful or harmless but that contains hidden code designed to exploit or damage the system on which it is run. Trojan horse programs are most commonly delivered to users through e-mail messages that misrepresent the program's purpose and function. Also called Trojan code.	43
Trusted Path	A communication link that has been certified to a specific level of security or risk avoidance.	10
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by software that is not trusted.	15
Trusted Path	A means by which a user and a TSF can communicate with necessary confidence to suppot the TSP. [ISO/IEC 15408-1: 1999]	42
Update	A broadly released fix for a specific problem addressing a noncritical, non-security-related bug.	43
Update	To make a system or data file more current.	43

Term	Definition	Source
Upgrade	A software package that replaces an installed version with a newer version of the same software. The upgrade process typically leaves existing customer data and preferences intact while replacing the existing software with the newer version.	43
Upgrade	To change to a newer, usually more powerful or sophisticated version.	43
User	An individual or process acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.	1, 10
User	Individual or (system) process authorized to access an information system.	12, 14, 15
User	In data processing, the person or client who makes use of a computer system.	33
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. [ISO/IEC 15408-1: 1999]	42
Utilities:	The supply of Electric Power, Water, Natural Gas, and telecommunications to a control facility	13
Utility	A generic term that, when qualified, identifies the business entity including all its operating and business functions; e.g., electric utility, gas utility, water utility, wastewater utility, pipeline utility.	10
Virtual Private Network	A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.	13
Virtual Private Network (VPN)	1. Restricted-use logical computer network that is constructed from the system resources of a physical network, e.g. by using encryption and/or by tunneling links of the virtual network across the real network. [ISO/IEC FDIS 18028-1: 2006-03-31] 2. A protected information-system (IS) link utilizing tunnelling, security controls (*see* information assurance), and end-point address translation giving the user the impression a dedicated line exists between nodes. [INFOSEC-99]	41
Virtual Private Network (VPN)	The extension of a private network that encompasses encapsulted, encrypted, and authenticated links across shared or public networks. VPN connections typically provide remote access and router-to-router connections to private networks over the Internet.	43
Virus	1. An unwanted program which places itself into other programs, which are shared among computer systems, and replicates itself. Note: A virus is usually manifested by a destructive or disruptive effect on the executable program that it affects. 2. Self-replicating, malicious program segment that attaches itself to an application program or	41

Term	Definition	Source
	other executable system component and leaves no obvious signs of its presence. [INFOSEC-99] [ATIS}	
Virus	Code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or data. Compare worm. See also the definition provided by the Virus Info Alliance (f-secure.com).	43
Vulnerability	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.	10
Vulnerability	Weakness in and information system. System security procedures, internal controls or implementation that could be exploited.	12
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.	14, 15
Vulnerability	1. A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy. [RFC2828] 2. A flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely effect an organization's operations or assets through a loss of confidentiality, integrity, or availability. [NIST] 3. A weakness of an asset or group of assets that can be exploited by one or more threats [ISO/IEC 13335-1:2004]	41
Vulnerability	A weakness of an asset or group of assets which can be exploited by one or more threats. [ISO/IEC PDTR 13335-1 (11/2001)] A weakness that can be exploited by one or more threats. [ISO/IEC DTR 15947 (10/2001)] A weakness of an asset or group of assets which can be exploited by a threat. [ISO/IEC 17799: 2000]	42
Vulnerability	Any weakness, administrative process or act, or physical exposure that makes a computer susceptible to exploit by a threat.	43
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.	12, 15
Vulnerability Assessment	Vulnerability assessment is the process of identifying and quantifying vulnerabilities in a system. The system being studied could be a physical facility like a nuclear power plant, a computer system, or a larger system (for example the communications infrastructure or water infrastructure of a region). Vulnerability assessment has many things in common with risk assessment. Assessments are typically performed	41

Term	Definition	Source
	according to the following steps: • Cataloguing assets and capabilities (resources) in a system • Assigning quantifiable value and importance to the resources • Identifying the vulnerabilities or potential threats to each resource • Mitigating or eliminating the most serious vulnerabilities for the most valuable resources When dealing with computers, vulnerability assessment is also known as "white hat hacking". [WIKI]	
Wide Area Network (WAN)	A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN. Note 1: WANs may include physical networks, such as Integrated Services Digital Networks (ISDNs), X.25 networks, and T1 networks. Note 2: A metropolitan area network (MAN) is a WAN that serves all the users in a metropolitan area. WANs may be nationwide or worldwide. [ATIS]	41
Wide Area Networks	A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.	13
Worm	1. A computer virus capable of disrupting a computer program. [After Weik '96] 2. A self-contained program that can propagate itself through systems or networks. Note: Worms are often designed to use up available resources such as storage or processing time. [ANSDIT] 3. [An] independent program that replicates from machine to machine across network connections, often clogging networks and computer systems as it spreads. [INFOSEC-99]	41
Worm	Self-propagating malicious code that can automatically distribute itself from one computer to another through network connections. A worm can take harmful action, such as consuming network or local system resources, possibly causing a denial of service attack. Compare virus.	43
Zeroization	A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of data.	1, 10
Zeroization	To erase all the data stored on a volume and reinitialize the format of the volume.	33

Definition of Acronyms

Acronym	Definition	Source
ACE	Area Control Error	34
ACE	Access Control Entry	43
DCS	Digital Control System	32
DCS	Distributed Control System	10, 11, 41
DCS	Disturbance Control Standard	34
DoS	Denial of Service	10, 41
DoS	Denial of Service Attack	43
HAZOP	Hazardous Operations	10
HAZOP	Hazard and Operability	32
MAC	Message Authentication Code	10, 42, 43
MAC	Media Access Control	15
PLC	Programmable Logic Controller	32, 33
RFC	Requests for Comments	10
RFC	Request for Collaboration	43
SCADA	Supervisory Control and Data Acquisition	32, 34, 41, 42
SCADA	Supervisory Control And Data Acquisition System	2, 10, 13
SSL	Secure Socket Layer	10, 41
SSL	Secure Sockets Layer	43
SYN	Synchronized sequence numbers. Synchronized control flag in TCP header used to indicate the start of the process to establish a TCP connection; also refers to the message containing the set control flag.	5
SYN	Synchronized sequence numbers	10
TLS	Transport Level Security	41
TLS	Transport Layer Security	43
WAN	Wide Area Network	32, 10, 41
WAN	Wide Area Networks	13